422 Rec'd PCT/PTO 24 AUG 2000

FORM PTO-1390 REV. 5-93	US DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEYS DOCKET NUMBER P00,1249
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLICATION NO. (if known, see 37 CFR 1.5) 09/623037

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE98/02949	**02 OCTOBER 1998**	**27 FEBRUARY 1998**

TITLE OF INVENTION
METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS NETWORK

APPLICANT(S) FOR DO/EO/US **MICHAEL GUNDLACH ET AL.**

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2)) - drawings attached.
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2) - drawings attached.
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; **(PTO 1449, Prior Art, Search Report).**
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. **(SEE ATTACHED ENVELOPE)**
13. ☒ Amendment "A" Prior to Action.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☒ A change of address letter attached to the Declaration.
16. ☒ Other items or information:
    a. ☒ Request for Approval of Drawing Modifications, 2 sheets of drawings, Figures 1-3.
    b. ☒ Appointment of Associate Power of Attorney.
    c. ☒ EXPRESS MAIL # EJ 220501633US dated August 24, 2000.

U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/623037	INTERNATIONAL APPLICATION NO. PCT/DE98/02949	ATTORNEY'S DOCKET NUMBER P00,1249

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO . . . . . $840.00 International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) . . $670.00 No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2) . . . . . $760.00 Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO . . . . . $970.00 International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) . . . . . $ 96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

Claims	Number Filed		Number Extra	Rate		
Total Claims	03	- 20 =	0	X $ 18.00	$	
Independent Claims	01	- 3 =	0	X $ 78.00	$	
Multiple Dependent Claims				$260.00 +	$	
TOTAL OF ABOVE CALCULATIONS =					$ 840.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)					$	
SUBTOTAL =					$ 840.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +					$	
TOTAL NATIONAL FEE =					$ 840.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). $40.00 per property +						
TOTAL FEES ENCLOSED =					$ 840.00	
					Amount to be refunded	$
					charged	$

a. ☒ A check in the amount of $ 840.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 501519. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

SCHIFF HARDIN & WAITE
Patent Department
6600 Sears Tower
Chicago, Illinois 60606-6473

Mark Bergner
SIGNATURE

Mark Bergner
NAME

45,877
Registration Number

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Mailing Label Number EJ 220501633US

Date of Deposit: August 24, 2000

I hereby certify that this correspondence is being deposited with the United States Postal "Express Mail Post Office to Addressee" service under 37 CFR 1.10(c) on the date indicated above and is addressed to:

BOX PCT
Assistant Commissioner for Patents
Washington DC 20231

Case Number: **P00,1249**
Applicant(s): **Michael Gundlach et al.**

International Application No.	**PCT/DE98/02949**
International Filing Date	**02 OCTOBER 1998**
Priority Date Claimed	**27 FEBRUARY 1998**

Title: METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS NETWORK

Enclosed are the following documents:
International application as filed, drawings attached;
English Translation, drawings attached;
Annexes;
Executed Declaration;
Change of Address form for Applicants' Representative;
PTO 1390 in duplicate;
Amendment "A" prior to action;
Information Disclosure Statement; PTO 1449, Search Report, References;
Submission of Drawing Modifications, 2 sheets of drawings, Figures 1-3;
Appointment of Associate Power of Attorney;

Fee: $ 840.00
Postcard.

(See attached envelope for Executed Assignment; PTO 1595; $40.00 filing fee; Postcard)

Signature of person mailing documents and fees

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

APPLICANT(S):	MICHAEL GUNDLACH ET AL.
ATTORNEY DOCKET NO.:	P00,1249
INTERNATIONAL APPLICATION NO:	PCT/DE98/02949
INTERNATIONAL FILING DATE:	02 OCTOBER 1998
INVENTION:	"METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS NETWORK"

Assistant Commissioner for Patents,
Washington D.C. 20231

AMENDMENT "A" PRIOR TO ACTION

Sir:

Applicants herewith amend the above-referenced PCT application, and request entry of the Amendment prior to examination on the United States Examination Phase.

IN THE SPECIFICATION:

On page 1:

cancel lines 1-3 and substitute the following

--SPECIFICATION

TITLE

"METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS NETWORK"

BACKGROUND OF THE INVENTION

Field of the Invention-- therefor;

in line 5, cancel "be it" and substitute --which may be-- therefor;

in lines 5-6, cancel "network proceeding" and substitute --network. This

network is accessed-- therefor;

in line 6, cancel "wherein it is necessary" and substitute --and the network requires one-- therefor;

in line 7, cancel "means of";

in line 8, cancel "Besides" and substitute --in addition-- therefor;

in line 9, cancel ",";

above line 12, insert --Description of the Related Art--;

cancel lines 12-13 and substitute --An intelligent network IN architecture offers services in a communication network to users of this network. These-- therefor;

in line 14, cancel "referred to as";

in line 18, cancel "has the" and substitute --stores-- therefor;

in line 19, cancel "stored", cancel "purposes of" and before "storing", insert --e.g.,--;

in line 20, after "nodes", insert --,--;

in line 23, after "in", insert --such--, and cancel "thereby";

in line 24, cancel "what is referred to as", and cancel "calling'. The" and substitute --calling' service, in which the-- therefor;

in line 25, cancel "hereby";

in line 27, cancel "for purposes of gaining" and substitute --to gain", and cancel "aforementioned" and substitute --this-- therefor; and

in line 28, before "when", insert --(e.g.,--, and cancel "got lost, for example" and substitute --is lost)-- therefor.

On page 2:

in line 1, after "example", insert --,--;

in line 4, after "all", insert --of--;

in line 5, after "i.e.", insert --,--;

in line 8, cancel "spy out" and substitute --inappropriately acquire-- therefor;

in line 9, cancel "spying out" and substitute --acquiring-- therefor, after "it", insert --by--, before "user", insert --authorized--, and cancel "with respect to the input" and substitute --entering it-- therefor;

in line 10, cancel "also" and substitute --or-- therefor, and after "monitoring", insert --;--;

above line 14, insert --SUMMARY OF THE INVENTION--;

cancel line 16 and substitute

-- This object is achieved by a method for securing access of a user to a service in an intelligent telecommunication network, comprising the steps of entering, by the user, an unambiguous digit sequence in a terminal device, the digit sequence being only known to the user of the service, encoding the digit sequence and an additional variable parameter using an encoding function which thus produces a function calculation result, transparently transmitting the function calculation result containing the digital sequence, using multi-frequency dial methods, in the communication network up to a central entity, and evaluating the transmitted digit sequence in the central entity and permitting the user to use the service if the evaluation is positive and if a previously transmitted digit sequence has not been received within a fixed time interval. -- therefor;

in line 20, cancel the first "the" and substitute --An-- therefor, and cancel the last "the" and substitute --an-- therefor;

in line 21, cancel "means" and substitute --way-- therefor;

in line 23, cancel "whereby" and substitute --in which-- therefor; and

in line 24, cancel "; vice versa" and substitute --from x; however-- therefor.

On page 3:

in line 1, after "this", insert --result--;

in line 2, after "sequence,", insert --and--, and after "signaling", insert --,--;

in line 3, after "nodes", insert --,--;

in line 8, cancel "," and substitute --using-- therefor;

in line 9, cancel "in the [sic]" and substitute --to the-- therefor;

in line 14, cancel "outlay" and substitute --expenditure-- therefor, and cancel "already present" and substitute --already-present-- therefor;

in line 15, cancel "already received" and substitute --already-received-- therefor;

in line 18, cancel "outlay" and substitute --expenditure-- therefor, and after "since" insert --they also required entry of--;

in line 19, cancel "previously had to be entered as well";

in line 20, cancel "This misuse is hitherto" and substitute --Misuse is-- therefor, and after "possible,", insert --even absent access to the credit card--;

in line 23, cancel "means of";

in line 24, cancel "In this case, the" and substitute --But with the inventive method-- therefor; and

in line 25, cancel "from the".

On page 4:

in line 1, cancel "Thereby, a tapping trial" and substitute --With such a scheme, a tapping attempt-- therefor, and after "example", insert --,--;

cancel line 4 and substitute

-- This object is also achieved by a device in a telecommunication network for utilizing services offered in this network, with a telecommunication terminal device, which makes it possible for a user, by means of an input device, to dial-up a service and to enter a digit sequence for the authentication, with at least one switching node that transparently forwards the service call and the digit sequence and with a central entity in this network, which evaluates the service call and which carries out an authentication of the user on the basis of the entered digit sequence, characterized in that an encoding device exists, with an input device for a digit sequence and with a calculation device for calculating a result from the mathematical function and the digit sequence and with an output device for

transmitting the calculated result as multi-frequency dial tone and the authentication digit sequence is entered into this device, is encoded there and the result of this encoding, in the multi-frequency dial tone, is transmitted via the terminal device into the network and the central entity carries out an authentication procedure before access to the dialed-up service in the intelligent network is allowed. -- therefor;

in line 6, cancel "thereby";

in line 7, cancel "of" and substitute --used by-- therefor;

in line 8, cancel "means" and substitute --way-- therefor;

eliminate the paragraph break at the end of lines 10 and 11;

in lines 15-16, cancel "this course of action" and substitute --the inventive method/device-- therefor;

in line 16, cancel "already" and cancel "number a longer period of" and substitute --digit sequence long--;

cancel lines 17-18 and substitute --before actual usage of the device, which prevents unauthorized observation of the digit sequence input. -- therefor;

cancel line 20 and substitute --Advantageous embodiments and developments are provided when a variable parameter provided to the encoding function is a time specification, is a random number, or is taken from a number sequence that can be calculated. Furthermore, the encoding function can be a single-step method, or a two-step method according to ITU X.509. The encoding function can also be a method according to RFC 1938 or a hash function.-- therefor;

in line 23, cancel "works" and substitute --elements-- therefor;

in line 24, cancel "named, wherein" and substitute --specified, in which--; therefor;

in line 26, after "present", insert --in such a network--;

in line 27, after "from", insert --the--; and

in line 28, cancel "imaginable" and substitute --usable-- therefor.

On page 5:

in line 1, cancel "here" and substitute --in these-- therefor;

in line 7, after "example", insert --,--;

in line 8, after "of", insert --an--, and cancel ". In this case," and substitute --, in which-- therefor, and cancel "on one hand";

in line 9, cancel "Further" and substitute --Furthermore-- therefor;

in line 11, cancel "synchronized otherwise" and substitute --otherwise synchronized-- therefor;

in line 13, cancel ", whereby" and substitute --in which-- therefor;

in line 14, cancel "up" and cancel "value" and substitute --values-- therefor;

in line 17, after "X.509", insert --Information Technology - Open Systems Interconnection - The Directory: Authentication Framework ITU-T Recommendation x.509, 11/93--;

in line 18, after "1938", insert --Request for comments: 1938, May 1996, A one-time password system, N. Haller, Bellcore, C. Metz, Kaman Sciences Corporation, --;

in line 23, cancel "MFV" and substitute --Multi-Frequency (MFV)-- therefor;

in line 25, cancel "means" and substitute --way-- therefor;

in line 27, cancel "and it" and substitute --, which-- therefor; and

in line 28, cancel "it" and substitute --two-step encoding-- therefor.

On page 6:

in line 1, cancel "A" and substitute --In two-step encoding, a-- therefor, and cancel "thereby ensues" and substitute --occurs-- therefor;

in line 2, after "pass", insert --occurs--;

in line 11, cancel "MVF [sic]" and substitute --MFV-- therefor;

in line 14, cancel ". It is thereby detected" and substitute --, which determines--;

in line 15, cancel "be" and cancel "detected" and substitute --determine-- therefor;

in line 20, cancel "." and substitute --, and if so,-- therefor;

in line 21, cancel "When this is the case";

in line 22, cancel "In the other case" and substitute --Otherwise-- therefor;

in line 23, cancel "means" and substitute --way-- therefor; and

in line 29, cancel ". Thus," and substitute --so that-- therefor.

On page 7:

in line 7, cancel the first "the" and substitute -, a-- therefor;

in line 9, cancel "In particular, the" and substitute --Particularly-- therefor, and cancel "." and substitute --,-- therefor;

in line 10, cancel "Particularly" and substitute --especially-- therefor;

in line 13, cancel "outlay" and substitute --expenditure-- therefor;

above line 15, insert --BRIEF DESCRIPTION OF THE DRAWINGS --;

cancel line 16;

in line 17, before "the generation", insert --is a block diagram showing-- therefor;

in line 19, before "the generation", insert --is a block diagram showing--, and before "ITU", insert --the--, and cancel "," and substitute --.-- therefor;

in line 21, before "the generation", insert --is a block diagram showing-- therefor, and before "ITU", insert --the--;

above line 24, insert --DESCRIPTION OF THE PREFERRED EMBODIMENTS--;

in line 24, after "entity", insert --service control point--;

in line 26, cancel "by means" and substitute --via-- therefor;

in line 28, cancel "En route,"; and

cancel line 29 and substitute --Switching centers (SSP) en route pass the encoded access code transparently-- therefor.

On page 8:

cancel line 1 and substitute --The access code could be inappropriately acquired via-- therefor;

in line 2, after "tapping", insert --at this point--;

in line 4, before "access", insert --expected--, and cancel "to be expected";

in line 5, cancel "made [sic]" and substitute --created which reflects-- therefor;

in line 6, after "correct and", insert --thus whether--;

in lines 5-6, cancel "as a result thereof";

in line 10, cancel "thereby";

in line 13, cancel "are co-encoded here" and substitute --may be co-encoded-- therefor;

in line 18, cancel "an";

in line 21, cancel "means" and substitute --way-- therefor; and

below line 22, insert

-- The above-described method is illustrative of the principles of the present invention. Numerous modifications and adaptions thereof will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.--.

Cancel page 9.

IN THE CLAIMS:

On substitute page 10:

line 1, replace "Patent claims" with --WHAT IS CLAIMED IS:--;

Please amend claims 1-3 as follows:

1. (Amended) A method [Method] for securing [the] access of a user to a service in an intelligent telecommunication network [(IN)], comprising the steps of:

[- whereby the access is secured by means of] entering, by said user, an unambiguous digit sequence [(PIN)] in a [the] terminal device [(KE), which], said digit sequence [(PIN) is] being only known to said [the] user of said [the] service[,];

encoding said digit sequence and an additional variable parameter using an encoding function which thus produces a function calculation result;

transparently transmitting said function calculation result containing said digital sequence [- and this digit sequence], using [by means of] multi-frequency dial methods, [is transparently transmitted] in said [the] communication network up to a central entity [instance (SCP) and is evaluated there,]; and

evaluating said transmitted digit sequence in said central entity and permitting said user to use said service if said evaluation is positive and if a previously transmitted said digit sequence has not been received within a fixed time interval.

[- the digit sequence is supplemented by at least one further, variable parameter prior to the transmission by the communication network and
- is encoded by means of a suitable encoding function (f), and
- the result of this function calculation (rpPIN) is transmitted to the central instance and
- the user can utilize the service when the access code has not yet been received within a fixed time interval.]

2. (Amended) A method [Method] according to [patent] claim 1, wherein said
[characterized in that]

[a] variable parameter is a selected from the group consisting of a time specification, [or] a random number, and a number [or is] taken from a number sequence that can be calculated.

3. (Amended) A method [Method] according to claim 1, wherein said [one of the previous patent claims,
characterized in that]

[the] encoding function is selected from the group consisting of a single-step method according to ITU X.509, [or] a two-step method according to [norm] ITU X.509, [or is] a method according to RFC 1938, and [or is] a hash function.

IN THE ABSTRACT

On page 14:

in line 4, cancel "be it" and substitute --which may be-- therefor, and after "radio network", insert --,--;

in line 5, cancel "It is thereby" and substitute --In this network, it is-- therefor;

in line 6, cancel "means of";

in line 7, cancel "Besides" and substitute --In addition-- therefor; and cancel line 11.

REMARKS

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment of claims 1-3 is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

Mark Bergner (Reg. No. 45,877)

Mark Bergner
SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
Chicago, Illinois 60606-6473
(312) 258-5779
Attorney for Applicant(s)

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

APPLICANT(S):	MICHAEL GUNDLACH ET AL.
ATTORNEY DOCKET NO.:	P00,1249
INTERNATIONAL APPLICATION NO:	PCT/DE98/02949
INTERNATIONAL FILING DATE:	02 OCTOBER 1998
INVENTION:	"METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS NETWORK"

Assistant Commissioner for Patents,
Washington D.C. 20231

REQUEST FOR APPROVAL OF DRAWING MODIFICATIONS

Sir:

Enclosed are copies of the drawings (Figures 1-3) showing in red the addition of labels to the elements depicted therein. Approval of the additions is respectfully requested.

Submitted by,

Mark Bergner (Reg. No. 45,877)

Mark Bergner
SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
Chicago, Illinois 60606-6473
(312) 258-5779
Attorney for Applicant(s)

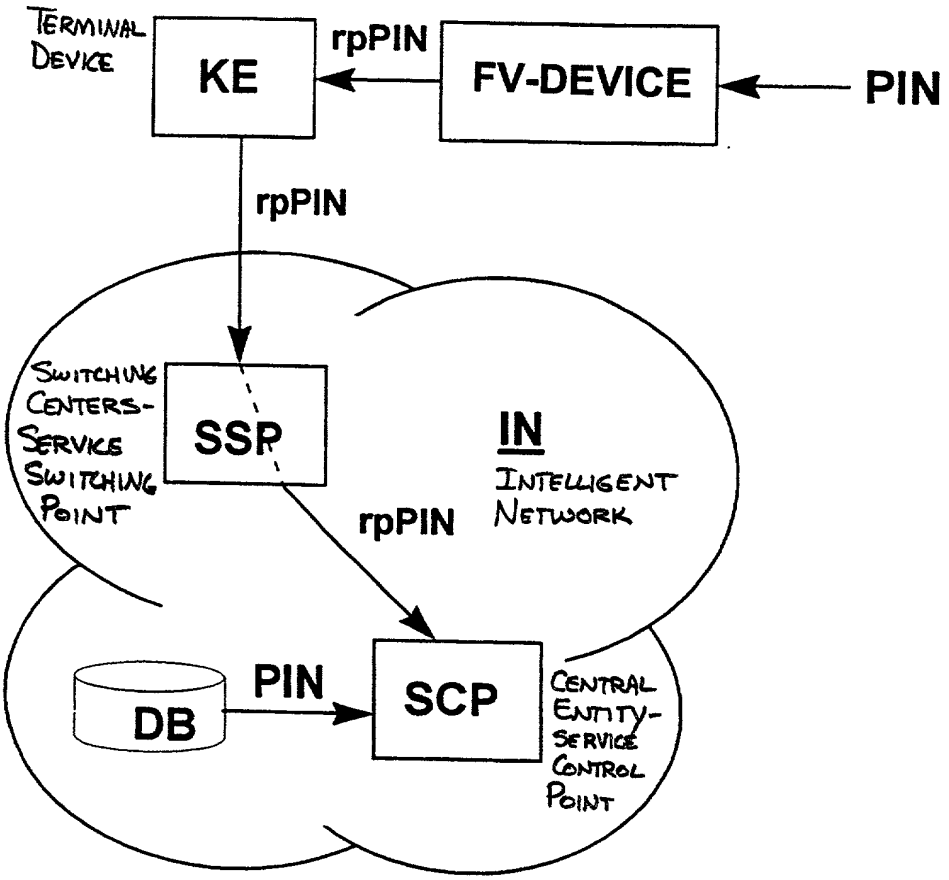

Fig. 1

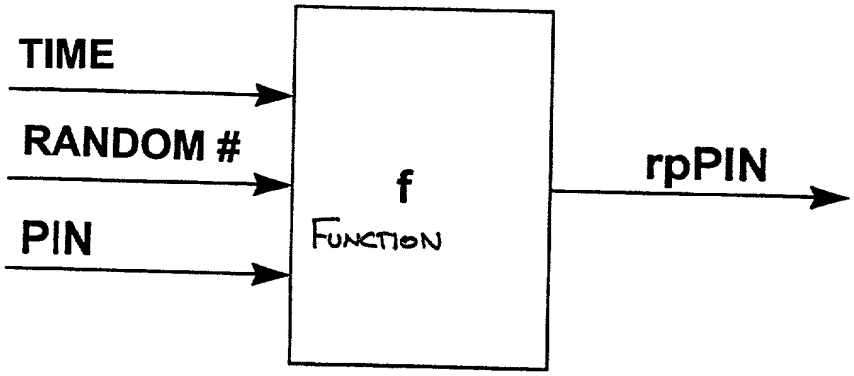

Fig. 2

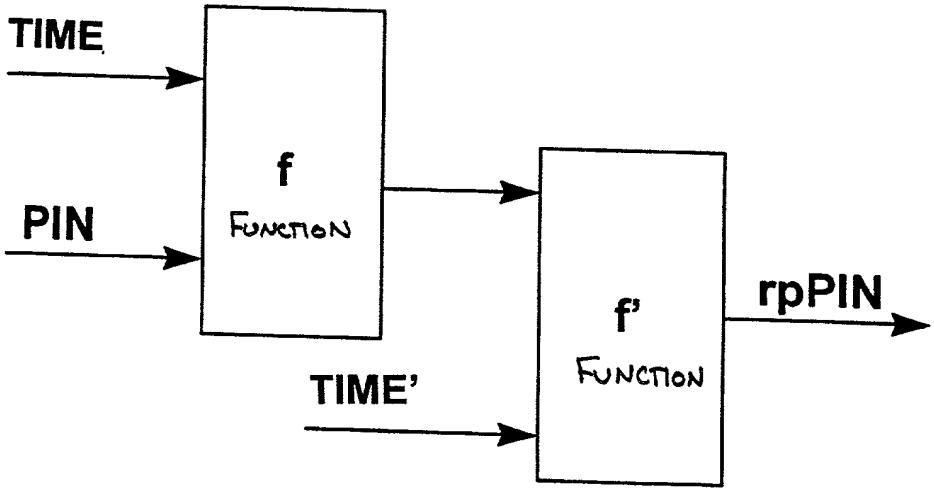

Fig. 3

METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATION NETWORK

The invention relates to a method for accessing a service in a telecommunication network, be it a private network, an intelligent network or a mobile radio network proceeding from an arbitrary communication terminal device, wherein it is necessary to authenticate oneself by means of entering digit sequences in order to receive access to a desired service. Besides, the invention relates to a device in a telecommunication network, which makes it possible to carry out a secure authentication of a user in the case of a service call.

Given an intelligent network IN, an architecture is concerned that makes it possible, in a communication network, to offer services to users of this network. These what are referred to as value-added services give network operators the opportunity to differentiate themselves from competitors and to develop additional income sources.

In order to be able to offer value-added services, the network operator needs at least one central node in his network (service control point), which has the bits of information stored that are necessary for purposes of carrying out the services (storing the service programs, forwarding to responsible network nodes etc.). This central node is also referred to as implementing entity.

The users in a communication network can thereby utilize interesting new services. One of the better known services is the what is referred to as 'credit card calling'. The caller is hereby charged via his credit card with the fees for actuated calls. Apart form the credit card number, the input of a private personal identification number (PIN) is also necessary for purposes of gaining access to the aforementioned service, so that there is no misuse when the credit card got lost, for example.

Such an access protection is also imaginable regarding other services, for example for users in a mobile network, a private network or a private virtual network.

In all these cases, the authenticating digit code is entered via the keyboard of the terminal device and is transparently (i.e. in plaintext) transmitted via the lines and switching nodes of the communication network.

There are two possibilities to spy out these access codes:

a) by spying-out the PIN, be it observing the user with respect to the input via the keyboard of his terminal device, also by video monitoring

b) by tapping the PIN with respect to the transmission between terminal device and the performing entity.

The invention is based on the object of proposing a possibility as to how the access to services in a telecommunication network can be fashioned more secure.

This object is achieved by means of a method according to patent claim 1.

The utilized method describes the following course of action:

the unambiguous digit sequence for securing the access is encoded subsequent to the input by means of an encoding function or a mathematical one-way function, which are known to someone skilled in the art.

A one-way function is a mathematical function f(x) = y, whereby y is simple to calculate; vice versa, the determination of x from y, on the other hand, is extremely complex and not necessarily unambiguous.

A further parameter is co-encoded, which changes with each new input of the digit sequence. Therefore, each new encoding process supplies a new result.

Together with the variable parameter, this is subsequently coded directly per protocol or is coded into a digit sequence, is sent in multi-frequency signaling potentially via switching nodes up to the central entity.
The transmission ensues in the same way as the previous process of the authentication.

Then, the central entity evaluates the transmitted digit sequence in that a result is also calculated from the known one-way function, the expected PIN and the co-supplied parameters and is compared in the [sic] received value.

The realization of this authentication method is comparatively simple. A sufficient number of encoding methods are known to someone skilled in the art. The implementation of the method is only necessary on the side of the user and at the central entity; the implementation outlay is low. An already present data bank can be simply expanded by a field for storing the already received access codes.

The advantage of the described method clearly lies in the protection of the user. The outlay is not greater for the user than in previous methods, since an access code previously had to be entered as well. However, an unauthorized user is efficiently prevented from calling at the expense of others. This misuse is hitherto possible, since it is not a precondition that the user also has the credit card when he enters the credit card number, for example. Thus, the access could be gained in a simple way by means of simply observing the entered number including PIN.
In this case, the lacking knowledge about the utilized encoding method additionally prevents from the unauthorized usage.

The access code is fashioned such that it is secure against tapping; one or more variable parameters are added, such as a specification about the point in time of the

request. Thereby, a tapping trial in the network (for example on the access line) becomes useless, since a repeatedly used access code is rejected in the first place.

This object is achieved by means of a device according to patent claim 9.

A device for purposes of encoding the entered PIN is thereby utilized. This device requires an input device (keyboard) similar to the one of the communication terminal device. The device converts the entered digit sequence by means of the mathematical one-way function, together with a variable parameter. Together with the second parameter, the result of the calculation is subsequently translated into multi-frequency signaling methods and is transmitted to the terminal device.
The transmission up to the central entity ensues from there.
The central entity carries out an authentication with the received access code.

In addition to the previously cited advantages, a critical advantage of this course of action is the possibility of being able to already enter the number a longer period of time before the actual usage. Thus, at least the 'spying-out' by means of observing the input of the number can be effectively prevented.

Advantageous embodiments and developments are provided in the subclaims.

The inventive course of action is particularly advantageous with respect to specific works of telecommunication networks. First of all, the architecture of the intelligent network is to be named, wherein, for example, the service 'credit card calling' has already been implemented. The infrastructure required for the method is already present. Apart from the private networks, which require a mechanism for accesses from outside, there is also the VPN - the 'Virtual Private Network', which is realized in IN technology as well. Finally, the method is also imaginable in communication

networks for mobile radio telephone service; here, the user must authenticate himself for a device as well.

A plurality of possibilities are imaginable for the variable parameters. In the most simple case, a random number is created each time; corresponding generator functions for random numbers are known to someone skilled in the art.
Another possibility is a time specification, for example a dividing in a time-slot pattern of arbitrary nature. In this case, the central entity, on one hand, can check whether the received access code is a current value. Further, the additional transmission of the variable parameter is potentially not necessary when the transmitter and the receiver are synchronized otherwise in terms of time.
Another possibility is the generation of a mathematical progression with an initial number n, whereby the sequence number n2 can result from its precursor number n1 in different ways, such as summing up a fixed value.

Numerous methods and functions are known to someone skilled in the art regarding the type of encoding. In particular, the ITU recommendation X.509 and the RFC 1938 represent different complex and secure authentication and encoding methods.

The ITU recommendation X.509 particulary represents two methods.
The first and more simple method only uses an encoding process. The one-way function f is applied to one or more variable parameters and the PIN, possibly expanded by a string that is known to the MFV transmitter and the telecommunication service. The result from f (parameter1, [parameter2, ...], PIN) is converted into a digit string, which is then transmitted by means of the MFV transmitter.

It is more complex to realize a two-step encoding and it also requires more computing power with respect to the transmitter and receiver; however, it also offers a significantly higher protection.

A first encoding step thereby ensues in the same way as the above cited, single-step method. Subsequently, a second pass with a second mathematical algorithm f' (which can be identical with the first function f); the result calculates as follows:
f' (parameter x1 [,parameter x2, ..], f (parameter y1 [,parameter y2], PIN), PIN.

A generalized encoding process requires the multiple application of one algorithm or of different algorithms, respectively with the input parameters PIN and additional variable parameters.

When the result of the encoding is not a numeric digit sequence, or when the result cannot be transmitted without MVF [sic] tones (as it is the case with respect to ISDN), the result must be translated in such a digit sequence prior to the transmission.

The authentication method checks the transmitted digit code. It is thereby detected whether the user is authorized to access a service. It can be additionally detected whether the digit code that is authorized to access a service is misused.

The authentication can proceed as follows:

- The central entity checks whether the sent access code has already been received once in a fixed time interval.
  When this is the case the authentication is discontinued as unsuccessful.
- In the other case, the central entity calculates the access code to be expected by means of the same one-way function and the second parameter contained in the received access code and compares the result to the received one. The authentication is successful when the calculated and received code match. The user is allowed to access the desired service.

It can be advantageous to integrate the encoding device into the communication terminal device. Thus, the user does not have a second device that can get lost.

Transmission errors of the encoding device to the terminal device are also avoided. A generator for MFV tones, which is already present in the terminal device, can be utilized and potentially modified.

The application possibilities of this method in a telecommunication network (particularly an intelligent network, a private network or a mobile network) are versatile. Particularly the fee aspect represents a critical factor not only for the service provider but also for the network user.
In particular, the credit card telephony is associated with an extremely high risk. Particularly since the extent of the damage does not become obvious before the next invoice, since a loss of the card is not noticed in the case of misuse.
Both sides can achieve an extremely high advantage with a comparatively small outlay.

The invention is subsequently explained on the basis of exemplary embodiments. Shown are

Figure 1 the generation, transmission and authentication of a one-time-access code in an intelligent network,

Figure 2 the generation of the one-time-access code according to ITU X,509, single-step method, and

Figure 3 the generation of the one-time-access code according to ITU X.509, two-step method.

Figure 1 shows the path of an access key (PIN) from a user up to a central entity (SCP) in an intelligent network.
Subsequent to the input in a device for purposes of encoding (MFV), the PIN is transmitted by means of dial tones to the terminal device (KE) and from there is transmitted into the communication network to the central entity (SCP). En route, switching centers (SSP) are passed via which the encoded access code is currently

transparently transmitted. The access code could hereby be spied out by means of tapping. The central entity (SCP) checks the access code on the basis of already known data, for example, from a data bank (DB), and the co-supplied data from the supplied digit string. After the access code to be expected has been calculated and compared to the received one, an acknowledgment message is made [sic] whether or not the transmitted access code is correct and the user is allowed access as a result thereof.

Figure 2 and Figure 3 schematically show the generation of an access code that is to be transmitted via the network to the central entity. A symmetrical key is thereby required (PIN), which is known to the user and the central entity, which carries out an authentication. The PIN itself is not transmitted in a decoded manner.

In addition, two variable parameters are co-encoded here - a time specification (time, time') and a random number. These components change with each authentication process and thus prevent a detected one-time-access code from being used again. When these components cannot be automatically derived with respect to the central entity, they must be co-transmitted during the authentication.

Additional data, such as an arbitrary text, can also be utilized for the formation of the one-time-access code. These data are either known to both sides or are derivable or are additionally transmitted.

An encoded access code (rpPIN) is generated by means of the one-way function f (and f').

Bibliography

ITU-T x.509
Information Technology - Open Systems Interconnection -
The Directory: Authentication Framework
ITU-T Recommendation x.509, 11/93

RFC 1938
Request for comments: 1938, May 1996
A one-time password system
N. Haller, Bellcore, C. Metz, Kaman Sciences Corporation

Abbreviation list

f, f'	mathematical functions
IN	intelligent network
ITU	international telecommunication union
KE	communication terminal device
MFV	multi-frequency method
PIN	personal identification number
rpPIN	replayprotected [sic]PIN
SCP	service control point
SSP	service switching point

ART 34 AMDT

Patent claims

1. Method for securing the access to a service in an intelligent telecommunication network (IN),

- whereby the access is secured by means of entering an unambiguous digit sequence (PIN) in the terminal device (KE), which digit sequence (PIN) is only known to the user of the service,
- and this digit sequence, by means of multi-frequency dial methods, is transparently transmitted in the communication network up to a central instance (SCP) and is evaluated there, and
- the digit sequence is supplemented by at least one further, variable parameter prior to the transmission by the communication network and
- is encoded by means of a suitable encoding function (f), and
- the result of this function calculation (rpPIN) is transmitted to the central instance and
- the user can utilize the service when the access code has not yet been received within a fixed time interval.

2. Method according to patent claim 1,
characterized in that
a variable parameter is a time specification or a random number or is taken from a number sequence that can be calculated.

3. Method according to one of the previous patent claims,
characterized in that
the encoding function is a single-step method or a two-step method according to norm ITU X.509, or is a method according to RFC 1938 or is a hash function.

Abstract

The invention relates to a method for accessing a service in a telecommunication network, be it an intelligent network, a private network or a mobile radio network from an arbitrary communication terminal device. It is thereby necessary to authenticate oneself by means of entering digit sequences in order to gain access to the desired service. Besides, the invention relates to a device in a telecommunication network that makes is possible to carry out a secure authentication of a user in the case of a service call.

Figure 1

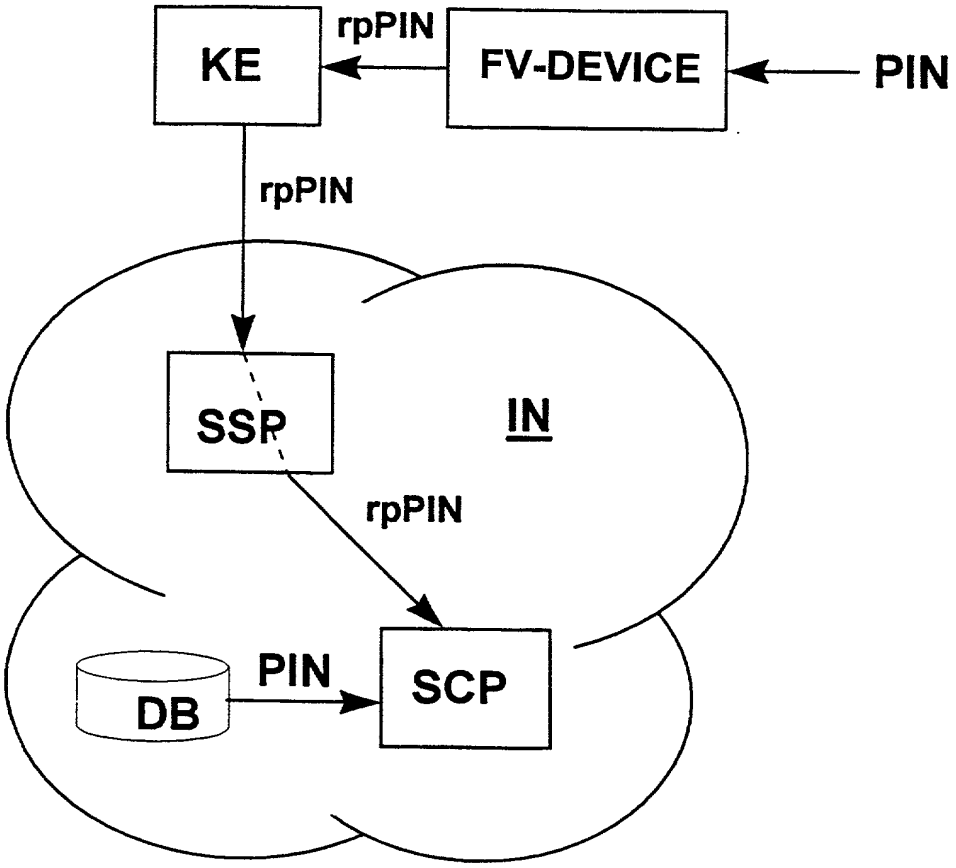

Fig. 1

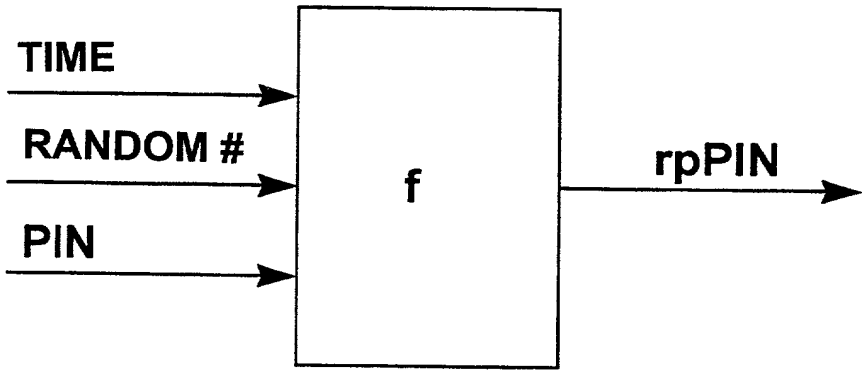

Fig. 2

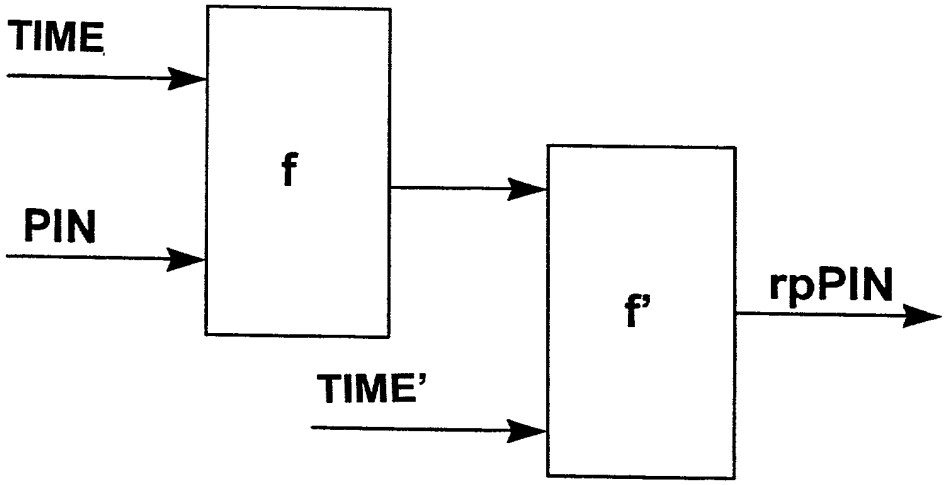

Fig. 3

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

APPLICANT(S):	MICHAEL GUNDLACH ET AL.
ATTORNEY DOCKET NO.:	P00,1249
INTERNATIONAL APPLICATION NO:	PCT/DE98/02949
INTERNATIONAL FILING DATE:	02 OCTOBER 1998
INVENTION:	METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS NETWORK

Assistant Commissioner for Patents,
Washington, D.C. 20231

APPOINTMENT OF ASSOCIATE POWER OF ATTORNEY

I am an attorney designated on the Power of Attorney for the above-referenced application. I hereby appoint Mark Bergner (Reg. No. 45,877) as an associate attorney, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Respectfully submitted,

(Reg. No. 31,870)
Melvin A. Robinson
SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
Chicago, IL 60606-6473
Attorney for Applicants

Declaration and Power of Attorney For Patent Application
Erklärung Für Patentanmeldungen Mit Vollmacht
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Verfahren und Vorrichtung zur Sicherung des Zugangs zu einem Dienst in einem Telekommunikations-Netz

deren Beschreibung

(zutreffendes ankreuzen)
☒ hier beigefügt ist.
☐ am _____ als
PCT internationale Anmeldung
PCT Anmeldungsnummer _____
eingereicht wurde und am _____
abgeändert wurde (falls tatsachlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

_____
_____
_____
_____

the specification of which

(check one)
☐ is attached hereto.
☐ was filed on _____ as
PCT international application
PCT Application No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Form PTO-FB-240 (8-83) Patent and Trademark Office-U.S. DEPARTMENT OF COMMERCE

German Language Declaration

Prior foreign appplications
Prioritat beansprucht

			Priority Claimed	
198 08 523.0	Germany	27. Februar 1998	☒	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			☐	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			☐	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgegeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

Messrs John D. Simpson (Registration No. 19,842) Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Guynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to. *(name and telephone number)*

312/876-0200
Ext. _____

Postanschrift:

Send Correspondence to:

HILL, STEADMAN & SIMPSON
A Professional Corporation
85th Floor Sears Tower, Chicago, Illinois 60606

Voller Name des einzigen oder ursprünglichen Erfinders: GUNDLACH, Michael	Full name of sole or first inventor:
Unterschrift des Erfinders Datum 1.10.98	Inventor's signature Date
Wohnsitz D-81739 München, Germany DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Vulpiusstr. 87 D-81739 München Bundesrepublik Deutschland	Post Office Addess
Voller Name des zweiten Miterfinders (falls zutreffend): NAUER, Bernhard	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum 27.8.98	Second Inventor's signature Date
Wohnsitz D-81373 München, Germany DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Fuggerstr. 4 D-81373 München Bundesrepublik Deutschland	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).